بسم الله الرحمن الرحيم

والحمد لله رب العالمين

والصلاة والسلام على سيدنا محمد النبي الكريم وعلى آله وأصحابه أجمعين

ربنا تقبل منا إنك أنت السميع العليم وتب علينا إنك أنت التواب الرحيم



يقول الله في كتابه العزيز

بسم الله الرحمن الرحيم

" وما أوتيتم من العلم إلا قليلا "

صدق الله العظيم

"رب أشرح لي صدري ويسر لي أمرى واحلل عقدة من لسانى يفقهوا قولي"

اللهم لا علم لنا إلا ما علمتنا إنك أنت العليم الحكيم

أخوكم في الله

م / مصطفى عبده توفيق محمد

جمهورية مصر العربية



Mostafa Digital

هجوم اليوم صفر

وكأن الفيروسات والديدان وبرمجيات التجسس التي نواجهها في حياتنا الحاسوبية اليوم ليست سيئة بما يكفي، ليأتينا هجوم اليوم صفر وينتشر أسرع من أي وقت مضى.

ما هو هجوم اليوم صفر؟

إنه فيروس أو برنامج خبيث كُتب حديثاً، كي يستغل ثغرة جديدة اكتشفت للتو في أحد البرامج أو في نظام التشغيل قبل أن يتمكن مطوِّرو البرمجيات من توفير ملف الإصلاح الخاص بها، أو حتى قبل أن يتم اكتشاف وجود الثغرة ذاتها.

و"اليوم صفر" هو ذلك اليوم الذي يتعرض فيه جهازك للإصابة، بعد أن تفتح أحد مرفقات البريد الإلكتروني المصابة أو تنقر على وصلة، وذلك لأن برنامج مكافحة الفيروسات وبرمجيات التجسس الذي تستخدمه، والذي تبذل قصارى جهدك في الحفاظ عليه محدَّثاً إياه حتى تاريخه، لا يعلم شيئاً عن هذا الهجوم الجديد.

عندما يجد الباحثون في المجال الأمني نقطة ضعف أو ثغرة في أحد أجزاء برنامج معين، فإنهم يعلنون ذلك، ثم تبدأ الشركات بالعمل لإصلاح المشكلة بأسرع ما يمكن. وتكون ملفات الإصلاح إما رقعاً أمنية من الجهة الأصلية التي أنتجت البرنامج، أو توقيعات (أي أجزاء صغيرة من الشيفرة تضم تعريفاً لهذه التهديدات ليتم تلافيها)، ثم يتم توزيع ملفات الإصلاح بسرعة.

لكن المؤسف أننا نشهد مزيداً من المرات التي ينتشر فيها الهجوم على نطاق واسع قبل طرح ملفات الإصلاح. إذ يكتشف بعض أصحاب القبعات السود (المخترقين) نقاط الضعف بأنفسهم، ويبدؤون باستغلالها حتى قبل أن تعلم عنها مايكروسوفت أو سيمانتك شيئاً. ويقول سامان أماراسينج، رئيس شركة البرمجيات الأمنية Determina: "مازالت هذه الهجمات نادرة نسبياً، لكنها تحدث". والأسوأ من ذلك أن الكثيرين يبدؤون بشن الهجمات على نقاط الضعف خلال ساعات قليلة بعد إعلان شركة مثل مايكروسوفت عن وجود نقاط الضعف هذه. وبينما كان كتاب الفيروسات يحتاجون في الماضي إلى حجم معين من الخبرة لاستغلال نقاط الضعف الجديدة في البرمجيات، فإنهم هذه الأيام ينعمون بوجود أدوات جاهزة يمكنهم استخدامها مباشرة، تستطيع فوراً أن تحول شيفرة رقعة إلى دودة أو فيروس.

من الأمثلة البسيطة على ذلك ما حدث في شهر آب/أغسطس 2005، عندما أعلنت مايكروسوفت عن وجود نقطة ضعف خطيرة في 'خدمة ركِّب وشغِّل' (Plug & Play Service)، ثم أطلقت رقعة أمنية لها في اليوم عينه. وخلال أسبوع ظهرت شيفرة تدَّعي إصلاح المشكلة وتستغل نقطة الضعف المعلن عنها، ثم تبعتها ست من الديدان الحقيقية، وتحديداً من عائلة Zotop، وعلى الرغم من أن ظهور تلك الديدان لا يبدو فورياً تماماً لكنه حدث في زمن أقل مما تحتاجه العديد من الشركات لتحدّث جميع أنظمتها التي تعاني من نقطة الضعف تلك.

وحيث أن Zotop والهجمات المرتبطة بها كانت ديداناً، كنّا نتوقع أن برمجيات مكافحة الفيروسات لدينا قادرة على حمايتنا في مواجهتها. لكن ترتيب العملية هنا أضــر أيــضاً بالعديد من المستخدمين: ففي الوقت الذي كانت تسعى فيه شركات مكافحة الفيروسات للحصول على عينة من الدودة وكتابة توقيع يعرِّفها، كي توزّع هــذه التواقيــع علــى المستخدمين، كانت لدى الدودة الوقت الكافي لتنتشر وتتوسع كما يحلو لها.

لكن إلى أي حد انتشرت؟
وإلى أي حد توسّعت؟

توجد مجموعة أبحاث مختصة بأمن الحواسيب في جامعة Otto-von-Guericke في مدينة ماجديبيرج الألمانية تدعى AV-Test (عنوانها على الشبكة www.av-test.org)، وهي تتابع ردود أفعال شركات مكافحة الفيروسات في مواجهة الديدان المختلفة. ووجدت هذه المجموعة أن قليلاً من شركات إنتاج برامج مكافحة الفيروسات قادرة على إصدار التواقيع اللازمة خلال ساعات، أما الشركات الأخرى فتستغرق وقتاً أطول لتقديم الإصلاحات، يصل في بعض الحالات إلى أكثر من يومين. وتصاب خلال هذا الوقت عشرات الآلاف من الأنظمة كما تقول شركة مكافحة الفيروسات Trend Micro.

كان ممكناً أن يكون الأمر أسوأ من ذلك، لولا أن المستخدمين الذين يملكون برامج جدران نارية محدَّثة استطاعوا حماية أنظمتهم من العديد من هذه الديدان، لأن تلك الجدران النارية تحجب الاتصالات التي تحاول أن تجريها البرامج المجهولة، أما الأجهزة المصابة فكان معظمها لا يتمتع بحماية أي جدار نار. وحتى من دون وجود توقيعات، استطاع العديد من برمجيات مكافحة الفيروسات منع بعض أو جميع الديدان من تنفيذ أعمالها باستخدام وسائل الكشف الذاتية (Heuristic)، التي تحاول فهم ما تحاول البرامج أن تفعله. ويعني ذلك أن البرمجيات تستخدم قواعد تفحص من خلالها سلوك البرنامج عينه عوضاً عن استخدام تواقيع معينة لمنع التهديدات. وينتشر أسلوبان من وسائل الكشف الذاتية، يدعى الأول "سبر الشيفرة" (Code Scanning)، وفيه يتم البحث داخل البرامج الجديدة عن الوسائل المعروفة لاستغلال نقاط الضعف الأمنية، بينما يعمل الثاني الذي يدعى "منع السلوك" (Behavior Blocking) على مراقبة ما تفعله البرامج فيوقف تصرفاتها غير المتوقعة.

ولاكتشف التهديدات الجديدة، فإن العديد من برامج مكافحة الفيروسات التقليدية أضاف نوعاً من أساليب الكشف الذاتي إلى طريقة الكشف المرتكزة على التواقيع، لكن نجحت في ذلك بنسب متفاوتة. ويستخدم قليل من المنتجات الجديدة أسلوباً غير تقليدياً يتجنب التواقيع ويعتمد فقط على طرائق الكشف الذاتي. ومع أن إهمال الطريقة المجربة للحماية ضد الفيروسات وغيرها من البرمجيات الخبيثة (أي التواقيع) يبدو أمراً غريباً، إلا أن هذه الطريقة غير التقليدية قد تعمل بشكل جيد. فعندما راقبت مجموعة AV-Test عمل برنامج باندا الذي يستخدم أداة TruPrevent لمراقبة السلوك، وجدت أن البرنامج تمكن من صد الديدان الست التي تستغل نقطة ضعف 'ركِّب وشغِّل'.

وحيث أن شركات الأمن تشهد تناقصاً في الوقت الفاصل بين اكتشاف نقطة الضعف وبدء الهجوم، وبوجود كل تلك الادعاءات الضخمة من قبل منتجي البرمجيات حول تأمين الحماية الكاملة للنظام حتى من دون البحث عن التواقيع، أجروا اختباراً لأربعة من البرمجيات التي تقوم بالحماية عبر "ترقّب - Proactive" التهديدات. وأظهرت اختباراتهم، إضافة إلى اختبارات AV-Test نتائج مختلطة. بل إن مطوِّري أدوات حجب السلوك أنفسهم ليسوا مستعدين لطلب إزالة برامج مكافحة الفيروسات التقليدية من الأجهزة، وهم يتحدثون عوضاً عن ذلك عن توافق برامجهم مع برامج مكافحة الفيروسات التي تعتمد على التواقيع.

ومازالوا يعارضون أن يقوم معظم المستخدمين بشراء منتج آخر لدعم برامج مكافحة الفيروسات التي يستخدمونها. ونعتقد أن على معظم الأشخاص شراء أطقم أمنية من جهة واحدة بدلاً من تجزئة حمايتهم إلى مضادات الفيروسات والجدران النارية ومضادات التطفل ومضادات برمجيات التجسس. وتتحرك باندا في الاتجاه الصحيح بإضافة أداة Truprevent إلى طقمها الأمني. ونتمنى أن يعمل منتجو الأطقم الأمنية الآخرون بتحسين أدوات الكشف الذاتي في منتجاتهم.

لكن المؤسف أن العدد المتزايد من تهديدات اليوم صفر يعني أنه حتى هذه الوسائل لن تكون كافية، وقد يكون الطريق الممكن للتغلب على ذلك هو وسائل الكشف الذاتي، ونأمل أن تنضج هذه الوسائل وتتحول بسرعة إلى برامج شائعة الاستخدام؛ وإلا قد يصبح هجوم اليوم صفر المقبل كارثة حقيقية.





أرجو أن تكونوا استفدتم بقراءة هذا الكتاب ولتدعوا الله لي بظهر الغيب

ولأي استفسار بالرجاء مراسلتي على الرابط التالي :-

E mail :- MostafaDigital@yahoo!.com

ولكم تحياتي

م/ مصطفى عبده توفيق محمد